MARICOPA COUNTY
HIPAA PRIVACY
POLICIES AND PROCEDURES

Effective April 14, 2003

Table of Contents

STATEMENT OF PURPOSE 4

PRIVACY OFFICER 4

PRIVACY PRACTICES 5

USES AND DISCLOSURES OF PHI 5

Uses and Disclosures to Carry Out Treatment, Payment, and Health Care Operations 6

USES AND DISCLOSURES OF PHI WITH AUTHORIZATION 7

Uses and Disclosures That Require You Be Given an Opportunity to Agree or Disagree Prior To the Use or Release 7

Uses and Disclosures for Which Consent, Authorization, or Opportunity to Object Is Not Required 7

Right to Request Restrictions on PHI Uses and Disclosures 9

Right to Inspect and Copy PHI 9

Right to Amend PHI 10

The Right to Receive an Accounting of PHI Disclosures 10

The Right to Receive a Paper copy of The Privacy Notice upon Request 11

SAFEGUARDS 11

ADMINISTRATIVE SAFEGUARDS 11

TECHNICAL SAFEGUARDS 12

PHYSICAL SAFEGUARDS 12

MINIMUM NECESSARY 13

RETENTION OF PHI 14

DOCUMENTATION 14

VERIFICATION OF INDENTITY 14

EDUCATION AND TRAINING 14

COMPLAINT PROCESS 15

MITIGATION PROCEDURES 16
DETECTION OF OFFENSES AND IMPLEMENTATION OF CORRECTIVE ACTIONS 16
Investigation and Corrective Actions: 16
Systematic Changes to Correct Violations: 16
DISCIPLINARY SANCTIONS 17
MODIFICATIONS TO HIPAA PRIVACY POLICIES AND PROCEDURES 17
HIPAA CHECKLIST FOR NEW EMPLOYEES 17
DEFINITIONS 18
Authorization 18
Business Associate 18
Covered Entity: 18
Individually Identifiable Health Information (IIHI) 18
Health Care Carrier 18
Privacy Officer: 19
Protected Health Information (PHI): 19
Third Party Administrator: 19
MARKETING PROTOCOL FOR HEALTH CARE BENEFITS 19

STATEMENT OF PURPOSE

On August 14, 2002, the U.S. Department of Health and Human Services (HHS) published final regulations for Standards for Privacy of Individually Identifiable Health Information (the Privacy Rule). The Rule was established to provide national standards for the protection and privacy of protected health information (PHI).

The purpose of this document is the establishment of the Health Insurance Portability and Accountability Act (HIPAA) Policies and Procedures for the Employee Health Initiatives Department (EHI) of Maricopa County (County). This policy is effective April 14, 2003. This document provides a comprehensive outline of what the EHI's responsibilities are in compliance with Federal HIPAA Privacy Regulations.

PRIVACY OFFICER

The Employee Health Initiatives Manager (Pat Vancil) serves as the Privacy Officer.

The Privacy Officer's primary responsibilities include:

- development of the HIPAA Privacy Policies and Procedures;
- oversight of the HIPAA Privacy Policies and Procedures implementation;
- preparation and oversight of distribution of the HIPAA Privacy Notice;
- development, coordination and participation in the education and training for EHI department staff;
- development of an atmosphere to encourage staff to report possible noncompliance by the County, health insurance carriers and/or Third Party Administrators (TPA);
- acting on matters related to privacy compliance. This includes the design and coordination of internal reviews and any needed corrective action (e.g., revisions to HIPAA Privacy Policies and Procedures, institution of additional training, etc.);
- coordination with the Workforce Management and Development Department for disciplinary sanctions associated with violations of the HIPAA Privacy Policies and Procedures;
- coordination of mitigating efforts in the event of a violation to the Privacy Rules; and

- periodic revision of the HIPAA Privacy Policies and Procedures as a result of changes of Federal law.

PRIVACY PRACTICES

Certain benefit programs administered through the Employee Health Initiatives Department are considered to be a Group Health Plan that is regulated by HIPAA.
.
Maricopa County offers a Group Health Plan (the "Plan"), which is a type of Health Plan, for eligible regular employees, certain contract employees, retirees, and COBRA participants.

The Plan is required by law to take reasonable steps to ensure the privacy of personally identifiable health information and to inform individuals about:

- the Plan's uses and disclosures of Protected Health Information (PHI)
- individual's rights with respect to his/her PHI;
- the Plan's duties with respect to PHI;
- individual's rights to file a complaint with the Plan and to the Secretary of the U.S. Department of Health and Human Services; and
- the person or office to contact for further information about the Plan's privacy practices

The term "Protected Health Information" ("PHI") includes all individually identifiable health information transmitted or maintained by the Plan whether oral, written, or electronic.

USES AND DISCLOSURES OF PHI

Upon request, the Plan is required to give an individual access to certain PHI in order to inspect and copy it.

Use and disclosure of PHI may be required by the Secretary of the U.S. Department of Health and Human Services to investigate or determine the Plan's compliance with the privacy regulations.

Uses and Disclosures to Carry Out Treatment, Payment, and Health Care Operations

The entities that provide coverage under the medical, prescription, behavioral health and substance abuse, dental, vision, flexible spending accounts, and COBRA plans may share your PHI for treatment purposes, to get paid for treatment, or to conduct health care operations. Many of these entities may provide individuals with their own Notice of Privacy Practices. Refer to Table A for a list of the current entities that provide the above coverage.

The Plan and/or its business associates may use PHI, without consent, authorization, or opportunity to agree or object, to carry out treatment, payment, and health care operations. For each business associate, the Plan has a written contract that contains terms to protect the privacy of PHI.

The Plan may also share information or allow the sharing of PHI with Maricopa County as the Plan Sponsor for plan administration functions. The Plan Sponsor has amended its plan documents to protect PHI as required by federal law.

Treatment is defined as the provision, coordination, or management of health care and related services. It also includes but is not limited to consultations and referrals between one or more of an individual's providers. In addition, providers may share information with each other. The Plan does not use PHI for treatment purposes.

Payment includes, but is not limited to, actions to make coverage determinations and payment (including billing, premium payment, claims management, subrogation, coordination of benefits, reviews for medical necessity and appropriateness of care and utilization review and pre-authorizations). For example, the Plan may tell a doctor (provider) whether an individual is eligible for coverage or what percentage of the bill will be paid by the Plan.

Health care operations include, but are not limited to, quality assessment and improvement, reviewing competence or qualifications of health care professionals, underwriting, premium rating, and other insurance activities relating to creating or renewing insurance contracts. It also includes disease management, case management, conducting or arranging for medical review, legal services and auditing functions including fraud and abuse compliance programs, business planning and development, business management and general administrative activities. For example, the Plan may use information about an individual's claims to determine compliance with physician-issued prescriptions, refer the individual to a disease or case management program, project future benefit costs or audit the accuracy of its claims processing functions.

USES AND DISCLOSURES OF PHI WITH AUTHORIZATION

Written authorization will be obtained before the Plan uses or discloses PHI for employer-related activities that include, but are not limited to, ombudsman activities such as resolving claims issue, fitness for duty examinations, short-term disability claims, return to work program, employee assistance plan, ergonomics evaluations, wellness programs, workers' compensations claims, and care received at an on-site pharmacy or medical clinic. The individual may revoke his/her authorization in writing, at anytime, to stop any future uses or disclosures.

Certain types of PHI, including PHI regarding communicable disease and HIV/AIDS, drug and alcohol abuse treatment, and evaluation and treatment for serious mental illness, may have additional protection under state or federal law. Written authorization is required in order to release this type of information.

Uses and Disclosures That Require You Be Given an Opportunity to Agree or Disagree Prior To the Use or Release

Disclosure of PHI to family members, other relatives, and your close friends is allowed if:

- the information is directly relevant to the family or friend's involvement with an individual's care or payment for that care, and
- the individual either has agreed to the disclosure or has been given an opportunity to object and has not objected.

Uses and Disclosures for Which Consent, Authorization, or Opportunity to Object Is Not Required

Use and disclosure of an individual's PHI is allowed without an individual's consent, authorization, or request under the following circumstances:

1. When required by law.

2. When authorized by law regarding when an individual has been exposed to a communicable disease or is at risk of spreading a disease or condition.

3. When authorized by law to report information about abuse, neglect, or domestic violence to public authorities if there exists a reasonable belief that an individual may

be a victim of abuse, neglect, or domestic violence. In such case, the Plan will promptly inform the individual that such a disclosure has been or will be made unless that notice could cause a risk or serious harm. For purposes of reporting child abuse or neglect, it is not necessary to inform the minor that such a disclosure has been or will be made. Disclosure may generally be made to the minor's parents or other representatives although there may be circumstances under federal or state law when the parents or other representatives may not be given access to the minor's PHI.

4. The Plan may disclose an individual's PHI to a public health oversight agency for oversight activities authorized by law. This includes uses or disclosures in civil, administrative or criminal investigations, inspections, and licensure or for disciplinary actions (for example, to investigate complaints against providers); and other activities necessary for appropriate oversight of government benefit programs (for example, to investigate health care fraud).

5. The Plan may disclose an individual's PHI when required for judicial or administrative proceedings. For example, an individual's PHI may be disclosed in response to a subpoena or discovery request provided certain conditions are met. One of those conditions is that satisfactory assurances must be given to the Plan that the requesting party has made a good faith attempt to provide written notice to the individual, and the notice provided sufficient information about the proceeding to permit the individual to raise an objection and no objections were raised or were resolved in favor of disclosure by the court or tribunal.

6. When required for law enforcement purposes (for example, to report certain types of wounds).

7. For law enforcement purposes, including for the purpose of identifying or locating a suspect, fugitive, material witness or missing person. Also, when disclosing information about an individual who is or is suspected to be a victim of a crime but only if the individual agrees to the disclosure or the covered entity is unable to obtain the individual's agreement because of emergency circumstances. Furthermore, the law enforcement official must represent that the information is not intended to be used against the individual, the immediate law enforcement activity would be materially and adversely affected by waiting to obtain the individual's agreement and disclosure is in the best interest of the individual as determined by the exercise of the Plan's best judgment.

8. When required to be given to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death or other duties as authorized by law. Also, disclosure is permitted to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent.

9. The Plan may use or disclose PHI for research, subject to conditions.

10. When consistent with applicable law and standards of ethical conduct if the Plan, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and the disclosure is to a person reasonably able to prevent or lessen the threat, including the target of the threat.

11. When authorized by and to the extent necessary to comply with workers' compensation or other similar programs established by law.

Except as otherwise indicated, uses and disclosures will be made only with an individual's written authorization subject to the individual's right to revoke such authorization.

Right to Request Restrictions on PHI Uses and Disclosures

An individual may request the Plan to restrict uses and disclosures of his/her PHI to carry out treatment, payment or health care operations, or to restrict uses and disclosures to family members, relatives, friends or other persons identified by the individual who are involved in the individual's care or payment for the individual's care. However, the Plan is not required to agree to such request.

The Plan will accommodate reasonable requests to receive communications of PHI by alternative means or at alternative locations. The individual or his/her personal representative will be required to request restrictions on uses and disclosures of his/her PHI. Such requests should be made in writing to the **Employee Health Initiatives Manager, at 301 S. 4th Ave., Suite B100, Phoenix, AZ 85003**.

Right to Inspect and Copy PHI

An individual has a right to inspect and obtain a copy of his/her PHI contained in a "designated record set," for as long as the Plan maintains the PHI. *"Protected Health Information"* (PHI) includes all individually identifiable health information transmitted or maintained by the Plan, regardless of form. *"Designated Record Set"* includes the medical records and billing records about individuals maintained by or for a covered health care provider; enrollment, payment, billing, claims adjudication and case or medical management record systems maintained by or for a health plan; or other information used in whole or in part by or for the covered entity to make decisions about individuals. Information used for quality control or peer review analyses and not used to make decisions about individuals is not in the designated record set. The requested information will be provided within 30 calendar days if the information is maintained on

site or within 60 calendar days if the information is maintained offsite. A single 30 calendar day extension is allowed if the Plan is unable to comply with the deadline. The individual or his/her personal representative will be required to request access to the PHI in the individual's designated record set. Requests for access to PHI should be made in writing to the **Employee Health Initiatives Manager, 301 S. 4th Ave. Suite B100, Phoenix, AZ 85003**. If access is denied, the individual or his/her personal representative will be provided with a written denial setting forth the basis for the denial, a description of how the individual may exercise those review rights and a description of how the individual may complain to the Secretary of the U.S. Department of Health and Human Services.

Right to Amend PHI

If an individual believes his/her PHI is erroneous or incomplete, the individual has the right to request the Plan to amend his/her PHI or a record about an individual in a designated record set for as long as the PHI is maintained in the designated record set. The individual must make this request in and provide a reason to support his/her request. The Plan has 60 calendar days after the request is made to act on the request. A single 30 calendar day extension is allowed if the Plan is unable to comply with the deadline. If the request is denied in whole or part, the Plan must provide the individual with a written denial that explains the basis for the denial. The individual or his/her personal representative may then submit a written statement disagreeing with the denial and have that statement included with any future disclosures of his/her PHI. Requests for amendment of PHI in a designated record set should be made in writing to the **Employee Health Initiatives Manager, 301 S. 4th Ave. Suite B100, Phoenix, AZ 85003**. The individual or his/her personal representative will be required to request amendment of the PHI in his/her designated record set in writing.

The Right to Receive an Accounting of PHI Disclosures

At an individual's request, the Plan will also provide the individual with an accounting of disclosures by the Plan of his/her PHI during the six years prior to the date of the request, but not before April 14, 2003. However, such accounting need not include PHI disclosures made: (1) to carry out treatment, payment or health care operations; (2) to individuals about their own PHI; (3) prior to the compliance date; or (4) based on an individual's written authorization. If the accounting cannot be provided within 60 calendar days, an additional 30 calendar days is allowed if the individual is given a written statement of the reasons for the delay and the date by which the accounting will be provided. If an individual requests more than one accounting within a 12-month period, the Plan will charge a reasonable, cost-based fee for each subsequent accounting.

The Right to Receive a Paper copy of The Privacy Notice upon Request

To obtain a paper copy of the Privacy Notice, contact the **Employee Health Initiatives Manager in writing at 301 S. 4th Ave., Suite B100, Phoenix, AZ 85003**.

The Plan is required by law to maintain the privacy of PHI and to provide individuals with notice of its legal duties and privacy practices. This is effective beginning April 14, 2003 and the Plan is required to comply with the terms of this notice. However, the Plan reserves the right to change its privacy practices and to apply the changes to any PHI received or maintained by the Plan prior to that date. If a privacy practice is changed, a revised version of the privacy notice will be provided to all participants for whom the Plan still maintains PHI. The notice will be distributed electronically via the Electronic Business Center (EBC) Intranet via an e*Nouncement and such revised notice will be available through the Employee Health Initiatives Home page. Any revised version of this notice will be distributed within 60 calendar days of the effective date of any material change to the uses or disclosures, the individuals rights, the duties of the Plan or other privacy practices stated in such notice.

SAFEGUARDS

ADMINISTRATIVE SAFEGUARDS

The County has trained its Employee Health Initiatives Department on the HIPAA Privacy Policies and Procedures. Those employees are required to use all reasonable measures to safeguard individuals' PHI. In addition, Business Associates Agreements are in place with those organizations with which there is communication regarding PHI.

The office suite of the Employee Health Initiatives Department has been re-designed twice specifically for the protection of an individual's PHI. The most recent re-design was completed effective September 22, 2008 and created Individual consultation offices in the anterior reception area of the suite. Visitors are greeted by a receptionist who triages the purpose of their visit. If personal consultation is requested or required, the receptionist contacts the appropriate EHI employee to escort the individual to a personal consultation office.

The EHI Department's work areas are accessible by electronic badge readers to ensure only EHI employees have access to the office suite.

The EHI Department is a separate and distinct department from the Workforce Management and Development Department (formerly the Human Resources Department). In this organizational structure, the Workforce Management and

Development Department is viewed as the “employer” and therefore has no access to the EHI Department or to any PHI retained by the EHI Department.

In the event that employees of other County departments have the need to attend a meeting with the EHI Department employees, such meeting is required to be conducted within the EHI Conference Room. Attendees are escorted to the Conference Room by the receptionist. Unescorted visitors are not allowed within the EHI Department’s work area.

The EHI Department has a dedicated facsimile machine to which only EHI personnel have access. To further secure sensitive documents, several employees within the Benefits Division of the EHI Department have electronic fax capability where faxes are received through their email box.

Access to the EHI Department is provided to maintenance workers during the day when staff are present. Such workers include cleaning staff and facility staff.

TECHNICAL SAFEGUARDS

The EHI department does not keep PHI in paper form. All group health plan enrollment information is kept in a imaging system. Access to the images is controlled by individual security level. Only those EHI employees with a need to know are granted access to these images.

Paper PHI received in the EHI Department is scanned into the imaging system and attached to the employee’s electronic benefits file. The paper information is then shredded and/or disposed of through a vendor who provides secure disposal services.

PHI is not to be kept on individual personal computers. It is to be kept on a secure HIPAA drive to which only select EHI personnel have access. PHI received via email is to be attached to the employee’s electronic benefits file and then deleted from the employee’s personal computer. This is done by turning the email into a “.tif” document, storing it on the HIPAA drive where it is accessed and attached to the employee’s benefit file.

PHYSICAL SAFEGUARDS

Automatic screensavers are to be set for two minute intervals from the cessation of desktop work. Employees in the EHI Department are required to lock their desktop when they leave the office suite work area.

Consultation office doors are kept closed when meeting with employees or a covered dependent to protect their conversation, which may involve PHI, from being overheard.

The cubicle configuration for the Benefits Division staff is designed for seated privacy. Additionally, a dropped “cloud” ceiling has been installed to control noise level.

MINIMUM NECESSARY

When using or disclosing PHI or when requesting PHI from another covered entity, the Health Plan will make reasonable efforts not to use, disclose or request more than the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request, taking into consideration practical and technological limitations. However, the minimum necessary standard will not apply in the following situations:

- disclosures to or requests by a health care provider for treatment;
- uses or disclosures made to the individual;
- disclosures made to the Secretary of the U.S. Department of Health and Human Services;
- uses or disclosures that are required by law; and
- uses or disclosures that are required for the Plan’s compliance with legal regulations.

Disclosure of PHI does not apply to information that has been de-identified. De-identified information is information that does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual. In addition, the Plan may use or disclose “summary health information” to the plan sponsor or business associates for obtaining premium bids or modifying, amending or terminating the group health plan, which summarizes the claims history, claims expenses or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan and from which identifying information has been deleted in accordance with HIPAA.

Any time PHI is requested by another covered entity, the County will make reasonable efforts to limit the use or disclosure to the minimum amount necessary to accomplish the intended purpose of the use, disclosure or request. For disclosures or requests that are out of the ordinary, the County’s Privacy Officer will review each disclosure individually to ensure that it is in compliance with the minimum amount necessary.

Routine and recurring disclosures include information regarding employee requests for assistance with medical billing or pharmacy issues that are to be coordinated by EHI staff acting as a liaison with the health carrier and the employee.

Communications between the County, health carriers, and Business Associates are to be made via telephone, facsimile, U.S. mail, secure email or a secure server. All communications will be limited to the minimum amount reasonably necessary to achieve the purpose of the disclosure.

RETENTION OF PHI

All records pertaining to PHI are retained indefinitely. Safeguard procedures as listed above for the protection of records are followed as detailed above.

DOCUMENTATION

The County will maintain the policies and procedures in written form. A copy of the policies and procedures will be posted in the Electronic Business Center. Any communications required to be in writing will be maintained either in writing or an electronic copy as documentation.

VERIFICATION OF INDENTITY

If the County is planning to disclose PHI, it will verify the identity of the person making the request, establish his/her authority to have access to the information, and obtain any corresponding documentation. In the event of personal knowledge of the requestor, that shall be considered adequate verification of identity.

EDUCATION AND TRAINING

All Employee Health Initiatives Department employees with access to PHI have been trained prior to the effective date of HIPAA Privacy regulations, April 14, 2004, on the County's HIPAA Privacy Policies and Procedures. All new employees who have access to PHI will be trained on the County's HIPAA Privacy Policies and Procedures within a reasonable period after orientation prior to granting security access to the data.

The County will update the HIPAA Privacy Policies and Procedures as needed to be in compliance with Federal regulations.

COMPLAINT PROCESS

If an individual believes that his/her privacy rights have been violated, the individual may complain to the Plan by writing to the Employee Health Initiatives Manager, 301 S. 4th Ave.., Suite B100, Phoenix, AZ 85003. The individual may file a written complaint, either on paper or electronically, by mail, fax, or e-mail with the Secretary of the Department of Health and Human Services. To obtain a copy of the complaint form or for more information about the Privacy Rule or how to file a complaint with Office for Civil Rights, contact any OCR office or the individual can go online to www.hhs.gov/ocr/hipaa. Mailing address: Office for Civil Rights, U.S. Department of Health & Human Services, 50 United Nations Plaza – Room 322, San Francisco, CA 94102, Telephone (415) 437-8310, Fax (415) 437-8329, TDD (415) 437-8311. Visit the HHS OCR Web site at www.os.dhhs.gov/ocr/hipaa for more formation. The Plan will not retaliate against the individual for filing a complaint.

If an individual has any questions regarding this information or the subjects addressed in it, he/she may contact the following individual: Employee Health Initiatives Manager, 301 S. 4th Ave., Suite B100, Phoenix, AZ 85003, telephone number (602) 506-1010, or electronic mail BenefitsService@mail.maricopa.gov.

The County is committed to complying with HIPAA Federal and State privacy laws and to correct any violations whenever they may occur in the organization. Each individual has the responsibility to report to the County's Privacy Officer, and/or to the County's Health Care Carriers, any activity that violates applicable privacy laws, rules, regulations or the County's HIPAA Privacy Policies and Procedures.

The County's Privacy Officer, Health Care Carriers and Third Party Administrators will assist individuals who have questions regarding their privacy rights or who want to report a privacy breach. Any individual may contact the County's Privacy Officer, or Health Care Carrier's Privacy Office and/or Third Party Administrator's Privacy Officer to file a complaint over a possible breach of privacy regulations. A log will be maintained of reported violations, the nature of any investigation and its results, including mitigation measures taken. Individuals also have the right to report violations to the Secretary of the Department of Health and Human Services.

The County will make every effort to maintain the confidentiality of the identity of any individual who reports possible violations, although there may be a point at which an individual's identity becomes known or must be revealed as a legal matter.

There will be no retaliation against an individual who reports a possible violation of: Federal or State privacy regulations, the County's HIPAA Privacy Policies and Procedures, or his or her privacy rights.

MITIGATION PROCEDURES

If a use or disclosure by the County or the County's business associate(s) would violate HIPAA Privacy regulations, the County will take prompt action to mitigate any damaging effects that the disclosure could have on a participant(s). The County's employees are required to report any violation that they observe, or learn of, to the County's Privacy Officer, so that the action to mitigate the damage, if any, can commence promptly.

DETECTION OF OFFENSES AND IMPLEMENTATION OF CORRECTIVE ACTIONS

The County and its business associates will immediately address any possible violations of HIPAA Privacy regulations and/or privacy procedures. The Privacy Officer will work with, if applicable, business associates to avoid future violations.

Investigation and Corrective Actions:

If the County receives a report of non-compliance, or the Privacy Officer or a business associate of the County discovers credible evidence of a violation, an investigation will immediately ensue. It is the County's and its business associates' policy to institute corrective action upon identification of a violation.

Systematic Changes to Correct Violations:

After a problem has been identified and corrected, the Privacy Officer and, if applicable, business associates of the County will review the circumstances to determine:

1) Whether similar problems have been identified elsewhere;

2) Whether modifications to the County's HIPAA Privacy Policies and Procedures and/or business associates' policies and procedures are necessary to prevent and detect other inappropriate conduct or violations of privacy rules and/or procedures.

DISCIPLINARY SANCTIONS

All violators of the HIPAA Privacy Policies and Procedures will be subject to disciplinary action. The precise discipline will depend on the nature and severity of the violation. Any employee who fails to comply with the County's HIPAA Privacy Policies and Procedures will be subject to discipline as established in the County's Personnel Rules and Regulations.

MODIFICATIONS TO HIPAA PRIVACY POLICIES AND PROCEDURES

Examples of when the HIPAA Privacy Policies and Procedures must be modified include the following:

- Notification is received from a broker, newsletter, or another source of a modification to Federal HIPAA laws.
- A flaw is found in the existing HIPAA Privacy Policies and Procedures.
- The carrier or TPA has made a change in its policy that will affect the HIPAA Privacy Policies and Procedures.

HIPAA CHECKLIST FOR NEW EMPLOYEES

The Employee Health Initiatives Department has certain responsibilities to ensure HIPAA compliance for newly hired employees. These responsibilities are:

- Providing the initial HIPAA Privacy Notice to any employee who is eligible to participate in a group health plan, regardless of whether the employee enrolls or not. The Notice will be posted on the Web site.
- Providing new employees with a copy of the HIPAA Privacy Policies and Procedures. These will also be posted on the Web site.

DEFINITIONS

Whenever used, the following terms have the following meaning unless a different meaning is clearly required by the context:

***Authorization*:** To allow use and disclosure of PHI for purposes other than treatment, payment or health care operations by both the covered entity requesting the information and a third party.

***Business Associate*:** A person (including a vendor or other entity) who is not an employee of the covered entity and either performs or assists in a function involving the use or disclosure of Individually Identifiable Health Information (IIHI) (including certain insurance functions, such as claims processing, data analysis, utilization review and billing) or provides certain services to the covered entity (including accounting, actuarial, administrative and legal) which includes the receipt or disclosure of IIHI. A covered entity may be a business associate of another covered entity.

Covered Entity: This consists of (1) health plans, which includes health, dental, vision, prescription drug insurers, HMOs, long-term care insurers and employer sponsored group health plans; (2) health care clearinghouses, an entity that processes non-standard information received from another entity into a standard format, including billing services; and (3) any health care provider who transmits health information in electronic form, including hospitals, physicians, dentists and other practitioners and providers of medical or health services.

***Individually Identifiable Health Information (IIHI)*:** Health information that is a subset of health information, including demographic information collected from an individual, and is (1) created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

***Health Care Carrier*:** A health care carrier is an individual or group plan that provides or pays for the cost of medical care. This includes the following in one or any combination: a group health plan, a health insurance issuer, an HMO, Part A or Part B of the Medicare program, the Medicaid program, an issuer of a Medicare supplemental policy, an issuer of a long-term care policy (excluding a nursing home fixed indemnity policy), an employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.

Privacy Officer: An employee of Maricopa County who has the responsibility of developing and implementing HIPAA Privacy Policies and Procedures to ensure the County's compliance with the Privacy Rule.

Protected Health Information (PHI): Individually identifiable health information that is transmitted by electronic media, maintained in any electronic medium, or transmitted or maintained in any other form or medium. PHI excludes individually identifiable health information in education records covered by the Family Educational Right and Privacy Act, and employment records held by a covered entity in its role as employer.

Third Party Administrator: An entity that may collect premiums, pay claims and/or provide administrative services to the County's group benefits program.

MARKETING PROTOCOL FOR HEALTH CARE BENEFITS

The procedures described below must be followed when providing census information to brokers or forwarding census information to carriers in order to market any of the following health care benefits:

- Medical
- Dental
- Vision
- Prescription Drug Coverage
- EAP
- Mental Health and Substance Abuse Benefits
- Long Term Care Benefits

All census data collected to market healthcare benefits must be limited to the following fields:

1. Date of Birth
2. Gender

3. Coverage Type

4. Coverage Tier

5. City, State and Zip code

The following identifying factors may **not** be provided when forwarding census information:

- Employee's Name
- Employee's Last Name
- Social Security Number
- Employee's ID Number (used by the employer and/or TPA or insurance carrier)
- Employee's full address